

## CLAIMS

1. A method of managing alerts issued by intrusion detection sensors (11a, 11b, 11c) of an information security system (1) including an alert management system (13), each alert being defined by an alert identifier and an alert content, which method is characterized in that it includes the following steps:
- associating with each of the alerts issued by the intrusion detection sensors (11a, 11b, 11c) a description including a conjunction of valued attributes belonging to attribute domains;
  - organizing the valued attributes belonging to each attribute domain into a taxonomic structure defining generalization relationships between said valued attributes, the plurality of attribute domains thus forming a plurality of taxonomic structures;
  - completing the description of each of said alerts with sets of values induced by the taxonomic structures on the basis of the valued attributes of said alerts to form complete alerts; and
  - storing said complete alerts in a logic file system (21) to enable them to be consulted.
2. A method according to claim 1, characterized in that complete alerts are consulted by successively interrogating and/or browsing said complete alerts so that the alert management system (13) responds to a request by supplying pertinent valued attributes enabling a subset of complete alerts to be distinguished in a set of complete alerts satisfying the request in order to enable said request to be refined.
3. A method according to claim 2, characterized in that the pertinent valued attributes assigned the highest priority are those that are most general, given the taxonomic structures.

4. A method according to either claim 2 or claim 3,  
characterized in that the alert management system (13)  
further responds to the request by supplying alert  
identifiers satisfying the request and whose description  
5 cannot be refined with respect to said request.
5. A method according to claim 1, characterized in that  
the alert identifier is a pair consisting of an  
identifier of the intrusion detection sensor (11a, 11b,  
10 11c) that produces the alert and an alert serial number  
assigned by said sensor.
6. A method according to claim 1, characterized in that  
the content of each alert includes a text message  
15 supplied by the corresponding intrusion detection sensor  
(11a, 11b, 11c).
7. A method according to any one of claims 1 to 6,  
characterized in that each valued attribute includes an  
20 attribute identifier and an attribute value.
8. A method according to claim 7, characterized in that  
each attribute identifier is associated with one of the  
following attribute domains: attack domain, attacker  
25 identity domain, victim identity domain, and attack date  
domain.
9. A method according to claim 1, characterized in that  
the description of a given alert is completed by  
30 recovering recursively from generalization relationships  
of the taxonomic structures a set including the more  
general valued attributes not already included in the  
description of another alert completed previously.
- 35 10. A method according to any one of claims 1 to 9,  
characterized in that the valued attributes in the

taxonomic structure are organized in accordance with an acyclic directed graph.

11. A computer program characterized in that it is  
5 designed to execute the method according to any one of  
claims 1 to 10 when it is executed by the alert  
management system (13).